(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－272925

(43)公開日　平成８年(1996)10月18日

(51)Int.Cl.⁶		識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｇ０６Ｋ	19/10			Ｇ０６Ｋ	19/00	Ｒ
	17/00				17/00	Ｔ
	19/07				19/00	Ｈ

審査請求　未請求　請求項の数４　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平7－71778

(22)出願日　平成７年(1995)３月29日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(71)出願人　391024515
三菱電機セミコンダクタソフトウエア株式会社
兵庫県伊丹市中央３丁目１番17号

(72)発明者　藤岡　宗三
伊丹市中央３丁目１番17号　三菱電機セミコンダクタソフトウエア株式会社内

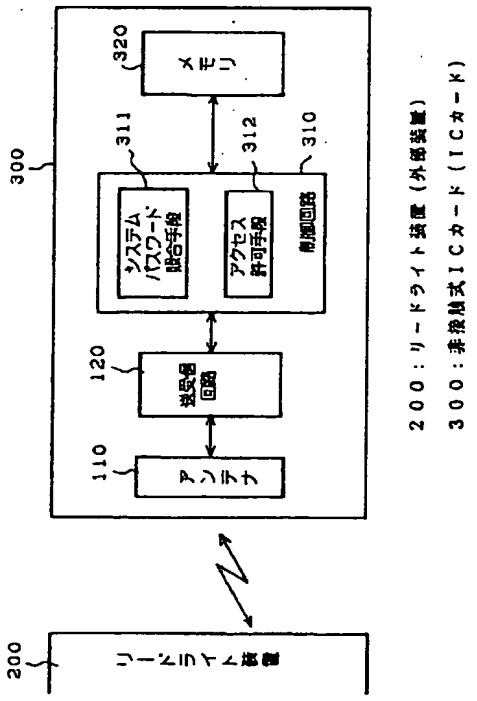
(74)代理人　弁理士　高田　守　（外４名）

(54)【発明の名称】　ＩＣカード

(57)【要約】

【目的】　テストを容易にできるＩＣカードを提供すること。

【構成】　メモリのシステムエリアにシステムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第１の情報が格納されている場合にはパスワード照合の結果、パスワードが一致しているときだけ外部装置からのシステムエリアのアクセスを許可する。システムエリアに第１の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可する。



1

【特許請求の範囲】

【請求項１】　外部装置との間で通信を行うＩＣカードにおいて、システムエリアとユーザエリアとに分割されているメモリであって、前記システムエリアは前記システムエリアを前記外部装置からアクセスするときに照合されるシステムパスワードを格納するためのシステムパスワード格納領域と、前記システムエリアをアクセスする場合に前記システムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第１の情報を格納するためのパスワード情報格納領域とを有するメモリと、前記メモリの前記パスワード情報格納領域に前記第１の情報が格納されている場合には、前記システムエリアを外部からアクセスする際に前記外部装置から送られてくるパスワードと前記システムパスワード格納領域に格納されているシステムパスワードとの照合を行うパスワード照合手段と、前記パスワード情報格納領域に前記第１の情報が格納されている場合には、前記パスワード照合手段の照合の結果パスワードが一致しているときだけ前記外部装置からのアクセスを許可し、前記パスワード情報格納領域に前記第１の情報が格納されていない場合には、パスワードの照合なしに前記外部装置からのアクセスを許可するアクセス許可手段とを具備することを特徴とするＩＣカード。

【請求項２】　前記システムエリアにはさらに前記ユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第２の情報を格納するための拡張システムエリア情報格納領域を有し、前記アクセス許可手段は前記拡張システムエリア情報格納領域に前記第２の情報が格納されている場合には、前記外部装置から前記拡張システムエリアがアクセスされる際に、前記パスワード照合手段の照合の結果、入力されたパスワードが前記システムパスワード格納領域に格納されているシステムパスワードと一致しているときに、前記外部装置からのアクセスを許可することを特徴とする請求項１記載のＩＣカード。

【請求項３】　前記拡張システムエリアは前記ユーザエリアをアクセスする場合に照合されるユーザエリアパスワードを格納するユーザエリアパスワード格納領域を有しており、前記ＩＣカードは、さらに、前記外部装置から前記ユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと前記拡張システムエリアに格納されているユーザエリアパスワードとを照合するユーザエリアパスワード照合手段を有し、前記アクセス許可手段は前記ユーザエリアパスワード照合手段による照合の結果、パスワードが一致した場合には、前記ユーザエリアに対する前記アクセスを許可することを特徴とする請求項２記載のＩＣカード。

【請求項４】　前記ユーザエリアパスワード格納領域には、前記外部装置からリードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワードと、前記外部装置からライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとが格納され、前記ユーザエリアパスワード照合手段は前記外部装置から入力されるコマンドの種類に基づいて前記リードパスワード、前記ライトパスワードのいずれかとパスワードの照合を行うことを特徴とする請求項３記載のＩＣカード。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明はプログラマブルなメモリを有し、電波等でデータ通信を行う非接触式のＩＣカードに関するものである。

【０００２】

【従来の技術】例えば、列車の定期券に非接触式ＩＣカードを用いて、改札口に備えられたリードライト装置との間でデータの転送をすることによって、その定期券が有効であるか否かをチェックするシステムが開発されつつある。

【０００３】図９は従来の非接触式ＩＣカードの構成を示すブロック図である。同図において、１００は非接触式ＩＣカード、２００は非接触式ＩＣカード１００と通信を行うリードライト装置、１１０はリードライト装置との間で電波の授受を行うために電気信号を電波に変換し、さらに電波を高周波信号に変換するアンテナ、１２０はアンテナ１１０によって変換された高周波信号をディジタル信号に変換し、ディジタル信号をアンテナ１１０に供給するための高周波信号に変換する送受信回路、１３０はデータを格納するメモリ、１４０は非接触式ＩＣカード１００の各部の制御を行うとともに非接触式ＩＣカード１００にデータの情報処理等を行う制御回路である。リードライト装置２００は非接触式ＩＣカード１００に電波によりコマンドを送り非接触式ＩＣカード１００はそのコマンドを実行し実行結果をリードライト装置２００に返送するように動作する。

【０００４】図１０はメモリ１３０の構成を示す図である。同図に示すようにメモリ１３０はシステムパスワードを格納する固定メモリ１３１とシステムエリアとユーザエリアに分割されているプログラマブルメモリ１３２とから構成されている。リードライト装置２００がシステムエリアのアクセスコマンドを非接触式ＩＣカード１００に送る場合にはコマンドにシステムパスワードを付加して送る。そして、このパスワードと非接触式ＩＣカード１００内の固定メモリ１３１に格納されているシステムパスワードとを照合し、一致したときのみアクセスできる。このためＩＣカードのメモリのテストを行う際も、システムエリアのテストはパスワードが必要なためテストが煩わしいという問題があった。さらに固定メモリ１３１にシステムパスワードが格納されているのでパスワードの変更が難しく、このためパスワードが破られた場合などに、その対応が難しいという問題があった。

【０００５】

【発明が解決しようとする課題】従来の非接触式ＩＣカードは、以上のように構成されているので、メモリのテストが煩わしく、さらにパスワードの変更が難しいなどの問題点があった。

【０００６】この発明は上記の問題点を解消するためになされたもので、メモリのテストが簡単にできるようにするとともにパスワードの変更も容易にできるＩＣカードを提供することを目的とする。

【０００７】

【課題を解決するための手段】請求項１の発明に係るＩＣカードは、システムエリアにシステムエリアを外部装置からアクセスするときに照合されるシステムパスワードを格納するためシステムパスワード格納領域と、システムエリアをアクセスする場合にシステムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第１の情報を格納するためのパスワード情報格納領域とを有するメモリと、パスワード情報格納領域に第１の情報が格納されている場合にはシステムエリアを外部からアクセスする際に外部装置から送られてくるパスワードとシステムパスワード格納領域に格納されているシステムパスワードとの照合を行うパスワード照合手段と、パスワード情報格納領域に第１の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第１の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可するアクセス許可手段とを具備したものである。

【０００８】請求項２の発明に係るＩＣカードは、請求項１の発明において、システムエリアにはさらにユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第２の情報を格納するための拡張システムエリア情報格納領域を有し、アクセス許可手段は拡張システムエリア情報格納領域に第２の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可する構成としたものである。

【０００９】請求項３の発明に係るＩＣカードは、請求項２の発明において、拡張システムエリアはユーザエリアをアクセスする場合に照合されるユーザエリアパスワードを格納するユーザエリアパスワード格納領域を有しており、ＩＣカードは、さらに、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合するユーザエリアパスワード照合手段を有し、アクセス許可手段はユーザエリアパスワード照合手段による照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可する構成としたものである。

【００１０】請求項４の発明に係るＩＣカードは、請求項３の発明において、ユーザエリアパスワード格納領域には、外部装置からリードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワードと、外部装置からライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとが格納され、ユーザエリアパスワード照合手段は外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行う構成としたものである。

【００１１】

【作用】請求項１の発明におけるアクセス許可手段は、パスワード情報格納領域に第１の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第１の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可する。

【００１２】請求項２の発明におけるアクセス許可手段は、拡張システムエリア情報格納領域に第２の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可する。

【００１３】請求項３の発明におけるユーザエリアパスワード照合手段は、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合し、アクセス許可手段はユーザエリアパスワード照合手段による照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可する。

【００１４】請求項４の発明におけるユーザエリアパスワード照合手段は外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行う。

【００１５】

【実施例】

実施例１．次に、この発明の一実施例を図について説明する。図１はこの発明の実施例１の非接触式ＩＣカードの構成を示す図である。なお、図９に示す従来の非接触式ＩＣカードと同一の部分には同一の符号を付し、重複する説明は省略する。図において、３００はこの実施例の非接触式ＩＣカード（ＩＣカード）、３１０は非接触式ＩＣカード３００の各部の制御を行うとともにデータの情報処理等を行う制御回路、３２０はデータを格納す

るためのプログラマブルのメモリである。

【００１６】図２はメモリ３２０のメモリマップを示す図である。同図に示すようにメモリ３２０はユーザエリアＵＡとシステムエリアＳＡとに分けられている。ユーザエリアＵＡは非接触式ＩＣカード３００を使用する人の個人情報や金額データなどアプリケーション用のデータとして使用するエリアである。システムエリアＳＡは非接触式ＩＣカード３００の制御のために使用するエリアである。システムエリアＳＡには、システムＩＤ、カードＩＤ、システムパスワード、及びシステムパスワードをシステムエリアＳＡに対して有効にするためのシステムパスワード有効コード（第１の情報）が格納される。システムパスワード有効コードがシステムパスワード有効コード格納エリアに格納されるとリードライト装置（外部装置）２００から非接触式ＩＣカード３００のリードライトのアクセスをするコマンドに付加されてきたパスワードがシステムエリアＳＡに格納されているシステムパスワードと一致した場合にのみシステムエリアのアクセスを行うことができるように構成されている。

【００１７】また、制御回路３１０にはリードライト装置２００からコマンドとともに送られてきたシステムパスワードをメモリ３２０のシステムエリアＳＡに格納されているシステムパスワードと比較するシステムパスワード照合手段３１１、及び、システムエリアＳＡのシステムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードが格納されており、かつ、送られてきたパスワードとシステムエリアＳＡに格納されているパスワードとが一致した場合にはリードライト装置２００からのアクセスを許可してコマンドを実行するアクセス許可手段３１２とを有している。なお、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コード（例えば、「Ｂ９Ｈ」）が格納されていない場合には、システムパスワードの照合の結果、パスワードが一致していなくてもリードライト装置２００からのアクセスは許可される。さらに、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードが格納されていない場合には、リードライト装置２００からパスワードなしでコマンドが入力された場合であっても、このコマンドはアクセス許可されて実行されるように構成されている。

【００１８】次に動作について説明する。リードライト装置２００が非接触式ＩＣカード３００のメモリ３２０のユーザエリアＵＡのデータをリードする場合、リードコマンドとリードアドレスとを電波として非接触式ＩＣカード３００に送る。非接触式ＩＣカード３００はアンテナ１１０で、送られてきた電波を高周波信号に変換し、送受信回路１２０で復調及びデコードを実行して制御回路３１０にリードコマンド及びリードアドレスを転送する。ユーザエリアＵＡのアクセスにはパスワードの照合は必要ないのでアクセス許可手段３１２によりリードコマンドは許可され、メモリ３２０のリードアドレスに対応するデータが読み出されて、送受信回路１２０及びアンテナ１１０を介してリードライト装置２００に電波として送出される。

【００１９】リードライト装置２００からデータを非接触式ＩＣカード３００にデータライトをする場合には、ライトコマンド、ライトアドレス、ライトデータを上述したデータのリードと同様にして電波として送出する。非接触式ＩＣカード３００では、データのリードの場合と同様に制御回路３１０にライトコマンド、ライトアドレス、ライトデータが転送される。ユーザエリアＵＡのアクセスにはパスワードの照合は必要ないのでアクセス許可手段３１２によりライトコマンドは許可され、メモリ３２０のライトアドレスにライトデータが書き込まれる。

【００２０】次にこの実施例の特徴的動作であるメモリ３２０のシステムエリアＳＡのアクセスについて説明する。リードライト装置２００から非接触式ＩＣカード３００のシステムエリアＳＡのリードライトはコマンドにパスワードを付加して非接触式ＩＣカード３００に送出する。非接触式ＩＣカード３００のシステムパスワード照合手段３１１は、まず、システムエリアＳＡのシステムパスワード有効コード格納エリアに特定のコードが格納されているかどうかを確認する。実際には、非接触式ＩＣカード３００が起動されるときに制御回路３１０に設けられているレジスタにシステムパスワード有効コード格納エリアのデータが転送され、このレジスタから出力される信号を参照して特定のコードが格納されているかどうかを確認する。このレジスタ等の構成については後に詳細に説明する。

【００２１】システムパスワード有効コード格納エリアに特定のコードが格納されていない場合にはシステムパスワードを付加せずにシステムエリアをアクセスすることができる。従って、リードライト装置２００からパスワードを付加せずにコマンドを送るだけで制御回路３１０のアクセス許可手段３１２はリード、ライト等のコマンドをユーザエリアＵＡのアクセスと同様に許可し、実行する。

【００２２】非接触式ＩＣカード３００の発行前に、メモリ３２０のテスト等を行う場合にはシステムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードを格納せずにシステムエリアＳＡをアクセスする。このようにすることでパスワードの照合を行うことなく、システムエリアＳＡをアクセスすることが可能になる。すなわち、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードを格納しない場合にはリードライト装置２００はシステムエリアＳＡをユーザエリアＵＡと同様にアクセスすることが可能になり、テストにかかる時間を短縮す

ることができる。

【００２３】特に、メモリ３２０の製造直後、すなわち、メモリのウエハ工程の終了直後はシステムパスワードが格納される領域の値がどのような値になっているかは不明であるのでシステムパスワードの照合なしにシステムエリアＳＡをアクセスできるようにすることは重要である。このため、メモリ３２０のシステムエリアＳＡのシステムパスワード有効コード格納エリアにはメモリのウエハ工程の終了直後になりやすいコード、「００Ｈ」、「０１Ｈ」、「０３Ｈ」、「０７Ｈ」、「０ＦＨ」、「１ＦＨ」、「３ＦＨ」、「７ＦＨ」、「ＦＦＨ」はさけることが望ましい。さらに、テストでメモリに書き込むコード、「００Ｈ」、「ＦＦＨ」、「５５Ｈ」、「ＡＡＨ」も避けることが望ましい。この実施例では「Ｂ９Ｈ」のコードを用いている。

【００２４】次に、テストが終了して、実際に非接触式ＩＣカード３００が発行される場合には、リードライト装置２００等からシステムパスワードの書き込みのコマンドを非接触式ＩＣカード３００に送出する。このコマンドに従って、非接触式ＩＣカード３００がシステムパスワードをシステムエリアＳＡにセットした後、リードライト装置２００等からシステムパスワード有効コード格納エリアに「Ｂ９Ｈ」を書き込むコマンドを非接触式ＩＣカード３００に送出する。このコマンドが実行されると、システムパスワードは有効になり、リードライト装置２００からシステムエリアＳＡをアクセスする場合には、システムパスワードの照合が必要になる。このため、発行された非接触式ＩＣカード３００ではセキュリティが保たれる。また、一旦発行された後でも、システムパスワードを知っていれば、システムパスワードを書き換えることも可能であり、一定期間ごとにシステム全体のパスワードを変更することによって極めて高いセキュリティを得ることが可能になる。

【００２５】次に、システムパスワード有効信号について説明する。図３はシステムパスワード有効信号ＳＰＥの発生回路を示す回路図である。同図において、３１４は非接触式ＩＣカード３００の起動時にシステムエリアＳＡのシステムパスワード有効コード格納エリアのデータが転送されて格納される８ビットレジスタ、３１５はこのレジスタ３１４が「Ｂ９Ｈ」になったときに「Ｈ」信号を出力するゲートである。非接触式ＩＣカード３００が起動される度にレジスタ３１４にはシステムパスワード有効コード格納エリアのデータがロードされる。そして、システムパスワード有効信号ＳＰＥは、システムパスワードが有効な場合にのみ「Ｈ」信号を出力する。従って、アクセス許可手段３１２はこのシステムパスワード有効信号ＳＰＥが「Ｌ」の場合はシステムエリアＳＡのアクセスにシステムパスワードの照合が不必要であると判断し、「Ｈ」の場合は、照合が必要であると判断する。

【００２６】図３に示すシステムパスワード有効信号の発生回路では８ビットのレジスタ３１４を用いたが、図４に示すように、１ビットのレジスタであるフリップフロップ３２１を用いるようにしても良い。この場合は、非接触式ＩＣカード３００の起動時にメモリ３２０のシステムパスワード有効コード格納エリアのデータをリードし、そのデータが「Ｂ９Ｈ」であったか否かがフリップフロップ３２１にセットされる。このフリップフロップ３２１の出力信号がシステムパスワード有効信号ＳＰＥとして用いられる。

【００２７】実施例２．図５はこの発明の実施例２の非接触式ＩＣカードの構成を示す図である。なお図１に示す非接触式ＩＣカードと同一の部分には同一の符号を付し、重複する説明は省略する。図において、３００ａはこの実施例の非接触式ＩＣカード（ＩＣカード）、３１０ａは非接触式ＩＣカード３００ａの各部の制御を行うとともにデータの情報処理等を行う制御回路である。

【００２８】図６はメモリ３２０のメモリマップを示す図である。なお、図２に示した部分と同一部分には同一の符号を付し、重複する説明は省略する。図６に示すように、メモリ３２０のアドレス０にはシステムエリアＳＡが設けられており、このエリアには図２に示すものに加えてシステムエリア拡張コード格納エリアが設けられている。このシステムエリア拡張コード格納エリアにシステムエリア拡張コード（第２の情報）を書き込むことによってアドレス１の拡張システムエリアＥＳＡがさらにシステムエリアとして確保されるように構成されている。拡張システムエリアＥＳＡには、リードパスワード（ユーザエリアパスワード）、リードパスワードリミットアドレス、ライトパスワード（ユーザエリアパスワード）、ライトパスワードリミットアドレスが格納される。リードパスワード、ライトパスワードは、それぞれ、ユーザエリアをリード、ライトする際に照合されるパスワードである。また、リードパスワードリミットアドレスはリードパスワードが有効となる上限のアドレスを示すものであり、ライトパスワードリミットアドレスはライトパスワードが有効となる上限のアドレスを示すものである。この実施例の場合にはリードパスワードリミットアドレスは１０、ライトパスワードリミットアドレスは５となっている。またこの実施例ではシステムパスワード有効コード格納エリアは７ビット、システムエリア拡張コード格納エリアは１ビットの領域となっている。

【００２９】図７はシステムパスワード有効信号ＳＰＥ及びシステム拡張信号ＳＸを生成する回路を示す図である。上述した実施例１では８ビットすべてをシステムパスワード有効コードを格納するために用いたが、この実施例ではＢＩＴ１からＢＩＴ７までの７ビットに、システムパスワード有効コード格納エリアのデータが、ＢＩＴ０にはシステムエリア拡張コード格納エリアのデータ

が、それぞれ、非接触式ＩＣカード３００ａの起動時にロードされる。３１７はゲートであり、レジスタ３１４に「Ｂ８Ｈ」または「Ｂ９Ｈ」が格納されている場合にシステムパスワード有効信号ＳＰＥとして「Ｈ」を出力する。さらに、３１６はゲートであり、レジスタ３１４に「Ｂ９Ｈ」が格納されている場合にのみシステム拡張信号ＳＸとして「Ｈ」信号を出力する。

【００３０】次に、この実施例の動作について説明する。まず、非接触式ＩＣカード３００ａのシステムエリアＳＡのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアとの領域に「Ｂ８Ｈ」を書き込んだ場合には、システム拡張信号ＳＸは「Ｌ」信号になり、システムパスワード有効信号ＳＰＥは「Ｈ」になる。この場合にはアドレス０のシステムエリアＳＡに対してのみシステムパスワードが有効になる。すなわち、システムエリアＳＡ以外の領域がユーザエリアＵＡ２として使用できる。この場合には実施例１と同様となり、ユーザエリアＵＡ２はパスワードなしでアクセスすることができ、システムエリアＳＡのアクセスはシステムパスワードの照合が必要になる。

【００３１】一方、システムエリアＳＡのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアとの領域に「Ｂ９Ｈ」を書き込んだ場合には、システム拡張信号ＳＸとシステムパスワード有効信号ＳＰＥのどちらも「Ｈ」信号になる。このため、図６に示すように、アドレス１の拡張システムエリアＥＳＡとシステムエリアＳＡのどちらに対してもシステムエリアＳＡに格納されているシステムパスワードが有効になる。すなわち、アクセス許可手段３１２はシステム拡張信号ＳＸ及びシステムパスワード有効信号ＳＰＥに基づいてシステムパスワード照合手段３１１によるシステムパスワードの照合が必要になるか否かを判断する。

【００３２】さらに、拡張システムエリアＥＳＡが確保された場合には、ユーザエリアＵＡ１は、拡張システムエリアＥＳＡに格納されるリードパスワード、リードパスワードリミットアドレス、ライトパスワード、ライトパスワードリミットアドレスを用いて、ユーザエリアパスワード照合手段３１３によってパスワードの照合が行われ、アクセス許可手段３１２によってパスワードとともに入力されたコマンドが許可さるか否かが判断される。ユーザエリアＵＡ１はアドレス２から１５までであるので、ライトパスワードの有効エリアはアドレス２から１０、リードパスワードの有効エリアはアドレス２から５になる。すなわち、アドレス２から５までのエリアはリード、ライトともにパスワードが必要になる。従って、このエリアには金額等の機密性の高いデータで発行後もリードライトすることが必要なデータを格納するのに適する。また、アドレス６から１０まではリードについてのみパスワードが必要になる。このため、住所、氏名、電話番号など発行後は読み出しだけですむデータを格納するのに適する。さらにアドレス１１から１５まではパスワードなしでアクセスすることが可能である。このため、セキュリティ不要のデータを格納するのに適する。このように、ライトパスワード、リードパスワードの２つのパスワードを設けることで、セキュリティのレベルの異なる３種類の領域に分割して管理することができる。また、リミットアドレスを変更することにより、それぞれの領域の大きさを変更することができ、メモリを効率よく管理して使用することが可能である。

【００３３】なお、図７では、システム拡張信号ＳＸとシステムパスワード有効信号ＳＰＥを生成するのに８ビットのレジスタ３１４を用いたが、図８に示すように１ビットのレジスタであるフリップフロップ３１８、３１９を用いて図４に示した場合と同様に出力されるシステム拡張信号ＳＸとシステムパスワード有効信号ＳＰＥを直接ラッチするようにしても良い。

【００３４】なお、システムエリアＳＡのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアに「Ｂ９Ｈ」、「Ｂ８Ｈ」以外のデータが格納されていた場合には、リードライト装置２００から入力されたコマンドはパスワードの照合なしに実行される。

【００３５】以上のように、この実施例では、拡張システムエリアをユーザエリアに確保できるとともに、ユーザエリアをリードパスワードとライトパスワードを用いてセキュリティを高くしてアクセスの管理を行うことができる。

【００３６】

【発明の効果】請求項１記載の発明によれば、パスワード情報格納領域にシステムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第１の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第１の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可するように構成したので、ＩＣカードのテストなどのときにはパスワードなしにアクセスできるのでテスト等の時間を短縮することができる効果がある。

【００３７】請求項２記載の発明によれば、拡張システムエリア情報格納領域に、ユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第２の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可するように構成したので、システムパスワードの有効となる範囲を可変することができ、多種のシステムに対応することができる効果がある。

【００３８】請求項３記載の発明によれば、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合し、照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可するように構成したので、ユーザエリアに対してもパスワードの照合によってセキュリティを向上させることができる効果がある。

【００３９】請求項４記載の発明によれば、ユーザエリアパスワード格納領域には、リードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワードと、ライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとを格納し、外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行うように構成したので、コマンドの種類に基づいて、効果的にユーザエリアをセキュリティ高く管理することができる効果がある。

【図面の簡単な説明】

【図１】　この発明の実施例１の非接触式ＩＣカードの構成を示す図である。

【図２】　図１に示す非接触式ＩＣカードのメモリのメモリマップを示す図である。

【図３】　実施例１における、８ビットのレジスタを用＊いたシステムパスワード有効信号の発生回路を示す図である。

【図４】　実施例１における、１つのフリップフロップを用いたシステムパスワード有効信号の発生回路を示す図である。

【図５】　この発明の実施例２の非接触式ＩＣカードの構成を示す図である。

【図６】　図５に示す非接触式ＩＣカードのメモリのメモリマップを示す図である。

【図７】　実施例２における、８ビットのレジスタを用いたシステムパスワード有効信号及びシステム拡張信号を生成する回路を示す図である。

【図８】　実施例２における、２つのフリップフロップを用いたシステムパスワード有効信号及びシステム拡張信号を生成する回路を示す図である。

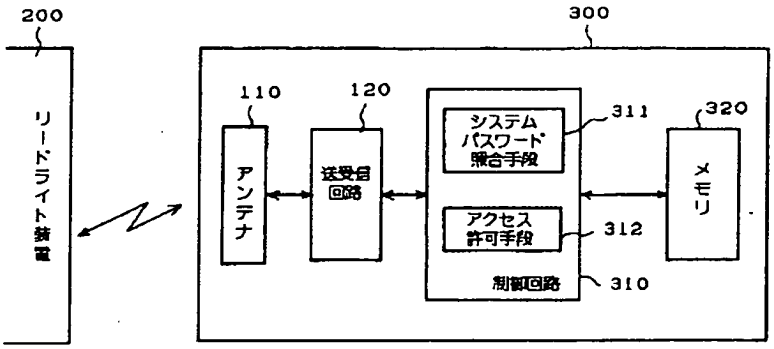
【図９】　従来の非接触式ＩＣカードの構成を示すブロック図である。

【図１０】　図９に示すメモリの構成を示す図である。

【符号の説明】

２００　リードライト装置（外部装置）、３００，３００ａ　非接触式ＩＣカード（ＩＣカード）、３１２　アクセス許可手段、３１３　ユーザエリアパスワード照合手段、３２０　メモリ。

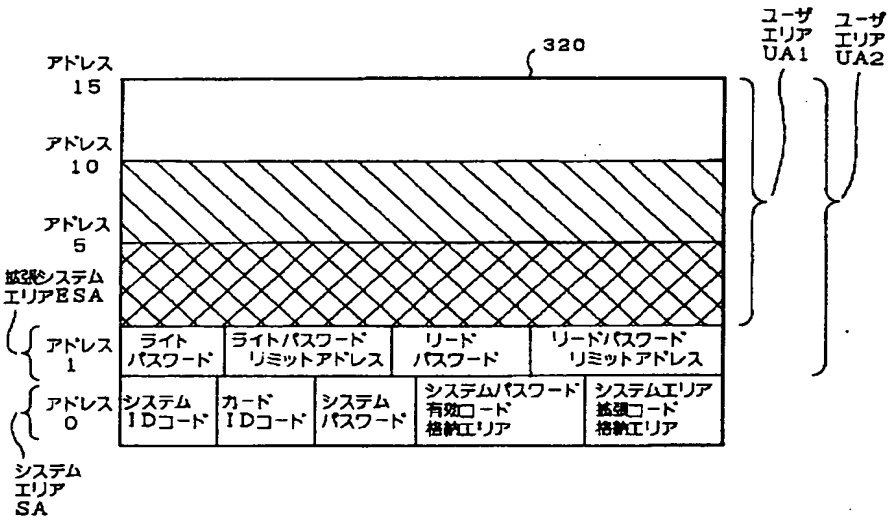
【図１】



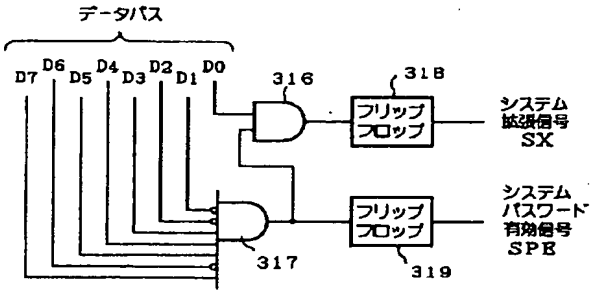
２００：リードライト装置（外部装置）

３００：非接触式ＩＣカード（ＩＣカード）

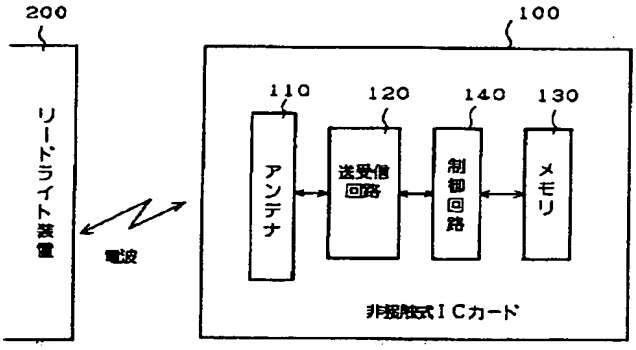
【図６】


320
ユーザエリアUA1
ユーザエリアUA2
アドレス15
アドレス10
アドレス5
拡張システムエリアESA
アドレス1
ライトパスワード
ライトパスワードリミットアドレス
リードパスワード
リードパスワードリミットアドレス
アドレス0
システムIDコード
カードIDコード
システムパスワード
システムパスワード有効コード格納エリア
システムエリア拡張コード格納エリア
システムエリアSA

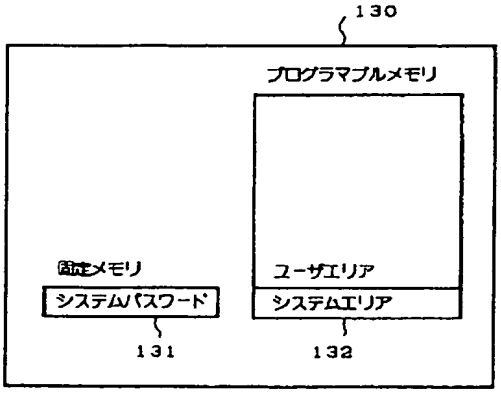
【図８】


データバス
D7 D6 D5 D4 D3 D2 D1 D0
316
318
フリップフロップ
システム拡張信号SX
317
319
フリップフロップ
システムパスワード有効信号SPE

【図９】


200
リードライト装置
電波
100
110
120
140
130
アンテナ
送受信回路
制御回路
メモリ
非接触式ＩＣカード

【図１０】


130
プログラマブルメモリ
固定メモリ
システムパスワード
131
ユーザエリア
システムエリア
132

US 096352170FP1

Creation date: 11-15-2004
Indexing Officer: ZBANGURA - ZAIN BANGURA
Team: OIPEBackFileIndexing
Dossier: 09635217

Legal Date: 01-20-2004

No.	Doccode	Number of pages
1	RCEX	1
2	A...	1
3	CLM	6
4	REM	4
5	XT/	1

Total number of pages: 13

Remarks:

Order of re-scan issued on .....